

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

ELECTRONIC DEVICES CURRENTLY LOCATED IN
THE EASTERN DISTRICT OF WISCONSIN)
)
)
)
)
)

Case No.

20-MJ-102

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Please see Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

Please see Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 841 and 846

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Mason J. Kohlhaas #247
 Applicant's signature

Mason Kohlhaas, FBI TFO
 Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/5/2020 @ 3:35 p.m.

William E. Duffin
 Judge's signature

City and State: Milwaukee, Wisconsin

William E. Duffin

U.S. Magistrate Judge

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
ELECTRONIC DEVICES CURRENTLY
LOCATED IN THE EASTERN DISTRICT
OF WISCONSIN

Case No. _____

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Mason J. Kohlhapp, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B, based at least in part on personal observations, knowledge and reports written by other law enforcement investigators, which I consider to be truthful and reliable.

2. I am a federally deputized Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI). I have been a FBI TFO with the Southeastern Wisconsin Regional Gang Task Force (SWRGTF) since March of 2019. During my (4) four years as a Deputy for the Milwaukee County Sheriff's Office, I have received training in the investigation of drug trafficking. I have participated in search warrants, investigations, and arrests in which controlled substances and drug paraphernalia were seized. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses. I have been involved in numerous narcotic and weapon based investigations, during which cellular devices

have been seized as evidence relating to narcotic distribution. I know through training and experience, as well through information obtained from other investigators that criminal drug traffickers use cellular devices to store and transmit information to others relating to ongoing criminal drug trafficking. I know that evidence of drug distribution can be found in the contact lists, photographs, videos, text messages, call logs, internet based applications, and other areas of digital storage within cellular devices that drug traffickers have in their possession.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched includes: (1) a black/red Verizon Kyocera flip phone with unknown serial number, (2) a blue/black Samsung Verizon flip phone with unknown serial number, (3) a black/red Verizon GZOne flip phone with unknown serial number, (4) an Apple iPhone 11 Pro with unknown serial number, and (5) an Apple iPhone 11 Pro Max with unknown serial number that are currently held as evidence inside the Federal Bureau of Investigation's Milwaukee Office at 3600 S Lake Drive, St. Francis, WI. Further property to be searched includes: (6) a black/red Kyocera flip phone with unknown serial number, (7) a black/gray Sprint Kyocera flip phone with unknown serial number, (8) a black/gray Verizon Samsung flip phone with unknown serial number, (9) a black/gray Samsung flip phone with unknown serial number, (10) an iPhone with case, unknown serial number, (11) a black/gray Samsung flip phone with unknown serial number/unknown carrier, and (12) an LG Smartphone with unknown serial number/unknown carrier, that are currently held as evidence inside of the Milwaukee Police Department's Property Division, located at 2620 W Wisconsin Avenue, Milwaukee, WI. The above mentioned electronic devices will be further referred to collectively as "the Devices."

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. In February of 2019, case agents initiated an investigation into a group of known and unknown drug traffickers operating in the Milwaukee area, known as the Buffum Meinecke Boys (“BMB”), including, Ramone LOCKE aka “Mone”, Amir LOCKE aka “Big Mir”, Joey VAZQUEZ aka “Joey”, Louis BATES aka “Little Louis”, Michael SMITH aka “M&M”, Garrell HUGHES aka “Rello”, Jesus PUENTES aka “JP”, Coury AGEE aka “Lil C”, Lamar JOHNSON aka “Fresh”, Luis LORENZO aka “Pito”, Victor GONZALEZ aka “Bey Bey”, and others. As part of the investigation, case agents have interviewed several confidential sources, conducted physical and electronic surveillance, utilized pen registers, reviewed historical phone toll records, reviewed subpoenaed records of documents, and have conducted controlled purchases of cocaine, crack cocaine, and heroin. As a result of the intelligence provided by the confidential sources and the controlled purchases, along with information obtained from other law enforcement techniques, case agents have identified various members of the BMB and identified several sources of supply.

7. Throughout the course of the investigation of BMB, case agents have made several controlled buys of controlled substances from members of BMB. Based on my training and experience, I know a “controlled buy” is a law enforcement operation in which an informant purchases drugs from a target. The operation is conducted using surveillance, usually audio and video taping equipment, and pre-recorded purchase money. When an informant is used, s/he is searched for contraband, weapons, and money before the operation. The informant is also wired with a concealed body recorder and/or a monitoring device. When the transaction is completed,

the informant meets case agents at a pre-determined meet location and gives the purchased drugs and the recording/monitoring equipment to the case agents. The informant is again searched for contraband, weapons, and money and then interviewed by the case agents about the drug transaction. A sample of the suspected drugs is then field tested by the case agents for the presence of controlled substances and then placed in inventory pursuant to normal inventory procedures. All of the calls to the target by the informants are consensually recorded calls under the direction and control of case agents and made in the presence of case agents. Additionally, case agents observe the informants dial the target's number on each occasion and the contact is verified through telephone records.

8. On January 2, 2020, case agents met with a particular confidential source hereinafter designated as CS # 3 to conduct a controlled purchase of heroin from Rico L. SMITH. CS #3 placed a consensually recorded telephone call to SMITH via 414.595.2473, where SMITH instructed CS #3 to Levels Nightclub, located at 634 West North Avenue, Milwaukee, Wisconsin. Law enforcement conducted surveillance observed CS #3 enter the nightclub and a short time later, observed Dennis KING walk into the nightclub. CS #3 exited a short time later and met with case agents. Surveillance observed KING exit the nightclub, walk to North 6th Street and West North Avenue, and entered the Honda Fit, bearing a Wisconsin registration plate of 244-ZTR, which was used by co-conspirators and KING in previous controlled buys. CS #3 stated that KING asked CS #3 if CS #3 was there for "Rico" (Rico SMITH); KING directed CS #3 to the bathroom of Levels and provided CS #3 with the suspected heroin, in exchange for the controlled buy money. CS #3 observed KING provide the controlled buy money to a patron of Levels, who CS #3 identified as SMITH's brother. Case agents conveyed the suspected heroin to the District Five Police Station and conducted a test

utilizing a Nark II 11 field test, which showed a positive result for opiates and fentanyl, with a weight of 50.98 grams.

9. Similarly, on December 20th, 2019, case agents met with CS #3 to conduct a controlled purchase of cocaine from Amir LOCKE. CS #3 conducted a consensually recorded telephone call to (414) 419-8956, where CS #3 spoke with LOCKE; LOCKE instructed CS #3 to travel to residence of the “lil bro”, who was later confirmed to be Alfonso D. GREER, aka “Goo.” CS #3 travelled to 1300 North Vel R. Phillips Avenue, Milwaukee, Wisconsin; waited in front of the loft complex; and a short time later, CS #3 travelled away from the area. CS #3 met with case agents at a predetermined meet location. CS #3 stated that “Goo” (GREER) exited the lobby of the loft complex, approached CS #3, and provided CS #3 with the suspected cocaine in exchange for the controlled buy money. CS #3 left the area and met with case agents at a predetermined location. Case agents conducted a search through law enforcement databases, where case agents determined that “Goo” was GREER. CS #3 was shown a photograph of GREER, which CS #3 positively identified as “Goo.” Case agents conveyed the suspected cocaine to the District Five Police Station and subjected a sample of the suspected cocaine to a Nark II 07 field test, which showed a positive result for cocaine, with a weight of 63.68 grams.

10. On February 19, 2020, a federal grand jury in this district returned an indictment charging multiple subjects -- including Rico SMITH, aka “Rico,” and Amir LOCKE, aka “Mir,” -- with knowingly and intentionally conspiring to distribute controlled substances, in violation of Title 21, United States Code, Sections 841 and 846, Case No. 20-cr-41.

11. On February 25, 2020, members of the Milwaukee Police Department and the Federal Bureau of Investigation responded to 4775 N Green Bay Avenue, in the City and County of Milwaukee, Wisconsin, and arrested Amir LOCKE, aka “Mir,” in connection with the federal

indictment described in paragraph 10. Law enforcement performed a search incident to arrest of LOCKE and his immediate area, recovering property including (4) an Apple iPhone 11 Pro, (5) an Apple Iphone 11 Pro Max, and a key fob for an Acura. LOCKE supplied consent for officers to search the 2017 white Acura MDX, with Wisconsin license plates of AHG-4782, that law enforcement knew LOCKE to operate. LOCKE knowingly, and without threat or promise, signed a consent form authorizing law enforcement investigators to search the above listed vehicle under his control. Law enforcement performed a consensual search of the vehicle parked in the parking lot of 4775 N Green Bay Avenue, Milwaukee WI, unlocking it with the keys obtained from LOCKE, and seized evidence from inside the vehicle, including (1) a red/black Verizon Kyocera flip phone with unknown serial number, (2) a blue/black Samsung Verizon flip phone with an unknown serial number, and (3) a black/red Verizon GZOne flip phone with unknown serial number. These five electronic devices were turned over and inventoried as evidence at the Federal Bureau of Investigation Milwaukee Office at 3600 S Lake Drive, St. Francis, Wisconsin.

12. On February 25th, 2020, law enforcement arrested Rico SMITH at 2853 N 5th Street, in the City and County of Milwaukee, Wisconsin, in connection with the federal indictment explained in paragraph 10. At the time, SMITH was operating a 2010 gray Infiniti G37 sedan, which he crashed in the course of evading arrest, near 2900 N 7th Street in the City and County of Milwaukee. A search of the vehicle was performed by law enforcement, during which various evidence was recovered, including (6) a black/red Kyocera flip phone with an unknown serial number, (7) a black/gray Sprint Kyocera flip phone with an unknown serial number, (8) a black/gray Verizon Samsung flip phone with an unknown serial number, (9) a black/gray Samsung flip phone with unknown serial number, (10) an Apple iPhone with case and

unknown serial number, and a (11) black/gray Samsung flip phone with unknown serial number/unknown carrier. A (12) LG Smartphone with unknown serial number/unknown carrier was recovered from SMITH'S person by investigators as part of a search incident to arrest. The devices obtained from SMITH's person and vehicle were inventoried as evidence with the Milwaukee Police Department and are currently being held at the Milwaukee Police Department's Property Control Division at 2620 W Wisconsin Avenue.

13. I know that persons who engage in ongoing criminal drug trafficking utilize cellular devices to further their activities. I know that drug traffickers utilize cellular devices to maintain contact with other affiliates and store information relating to drug trafficking. I know that evidence of drug trafficking can be held on the photographs, videos, call logs, text messages, contact lists, and otherwise stored digital information. I know that drug traffickers often record images and/or videos depicting narcotic evidence, maintain contact with others regarding drug trafficking through cellular devices which would be recorded in call logs and text messages, as well as maintain a contact list of affiliates within their cellular devices for personal reference and use. I know that additional evidence of drug trafficking would be stored within other digital stored memory of the cellular devices, and that law enforcement investigators could retrieve the electronically stored evidence if accessible.

14. The Devices are currently in the lawful possession of the Federal Bureau of Investigation (1-5) and the Milwaukee Police Department (6-12). Therefore, while the Federal Bureau of Investigation and the Milwaukee Police Department might already have all necessary authority to examine the devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

15. Based on my training and experience and work with fellow law enforcement, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of the the Federal Bureau of Investigation and the Milwaukee Police Department.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers and devices on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- f. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- g. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

17. Based on my training, experience, knowledge and research, I know that the Devices may have the capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training, experience, knowledge, and research, I have learned that examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices, like the Devices at issue here, can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a devices can also indicate who has used or controlled the devices. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement’s possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched includes: (1) a black/red Verizon Kyocera flip phone with unknown serial number, (2) a blue/black Samsung Verizon flip phone with unknown serial number, (3) a black/red Verizon GZOne flip phone with unknown serial number, (4) an Apple iPhone 11 Pro with unknown serial number, and (5) an Apple iPhone 11 Pro Max with unknown serial number, that are currently held as evidence inside the Federal Bureau of Investigation's Milwaukee Office at 3600 S Lake Drive, St. Francis, WI. Further property to be searched includes: (6) a black/red Kyocera flip phone with unknown serial number, (7) a black/gray Sprint Kyocera flip phone with unknown serial number, (8) a black/gray Verizon Samsung flip phone with unknown serial number, (9) a black/gray Samsung flip phone with unknown serial number, (10) an iPhone with case, unknown serial number, (11) a black/gray Samsung flip phone with unknown serial number/unknown carrier, and (12) an LG Smartphone with unknown serial number/unknown carrier, that are currently held as evidence inside of the Milwaukee Police Department's Property Division, located at 2620 W Wisconsin Avenue, Milwaukee, WI.

This warrant Authorizes the forensic examination of the Devices for the purposes of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 846, including but not limited to:
 - a. lists of customers and related identifying information;
 - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - d. any information recording the schedule or travel of Rico SMITH or Amir LOCKE;
 - e. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:
 - a. records of Internet Protocol addresses used;
 - b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review